We claim:

1. A method of generating a digital signature implemented over an elliptic curve public key encryption scheme utilizing information maintained secret in one computing device comprising the steps of

(i) initiating the computation of a coordinate a point on the elliptic curve from a pair of other points on said curve by performing on said one device an initial set of sufficient steps in the computation to inhibit recognition of information pertaining to the identity of said other points,

(ii) transferring to another computing device remote from the one device the results of said steps,

(iii) performing at least such additional steps in said computation at said other device to permit the completion of said computation at said one device, and

(iv) transferring the result of said additional steps to said one device for incorporation in said signature.

2. A method according to claim 1 wherein said initial steps includes a field operation to combine information from each of said other points.

3. A method according to claim 2 wherein said combined information is utilized in said additional steps.

4. A method according to claim 3 wherein said field operation includes the summation of the information representing one coordinate of each of said other points and the summation of the information representing the other coordinate of each of the other points.

5. A method according to claim 1 wherein said additional steps complete said computation.

09507117.042402

6. A method according to claim 4 wherein said information representing the summation of said coordinates is transferred from said one device to said other device.

7. A method according to claim 4 wherein said elliptic curve is over the finite field 2^m and represents said coordinates in a normal basis in said field.

8. A method according to claim 7 wherein said additional steps includes cyclically shifting said information representing the summation of said coordinates.

9. A method according to claim 1 wherein said computation generates a single coordinate of said point, said single coordinates being utilized in said signing.

10. A method of deriving a coordinate of a point on an anomalous elliptic curve over the field $GF2^m$ for utilization in a public key encryption scheme implemented on said curve, said method comprising the steps of

(i) storing a normal basis representation of each of a set of coordinates of points on said curve,

(ii) retrieving said normal basis representation of a coordinate of one of said points;

(iii) performing an i-fold cyclic shift on said retrieved normal basis representation of said one coordinate, and

(iv) utilizing the resultant representation as a coordinate of a further point on the curve resulting from an i-fold application of the Frobenius Operator to said one point.

11. A method according to claim 10 wherein each of said set of coordinates represents a point on the curve that is an integer multiple k, of a starting point P, and the i-fold application of the Frobenius Operation to said staring point P produces a new point $\varnothing^i P$ where $\varnothing^i P = \lambda^i P$,

said method including the step of determining the integer k' associated with said further point by computing $k\lambda^i$.

12. A method of generating a session pair k,kP for use in a digital signature performed on an anomalous elliptic curve in the filed $GF2^m$ where kP is a point on said curve resulting from the k fold addition of a starting point P where k is an integer, said method comprising the steps of

(i) storing a set of initial values of k and kP, as a normal basis representation in the field $GF2^m$,

(ii) selecting a coordinate of one of said points kP in said set of initial values;

(iii) performing an i-fold cyclic shift on said coordinate to obtain a normal basis representation of the coordinate after an i-fold application of a Frobenius Operator;

(iv) selecting the integer k associated with said one of said points;

(v) computing an integer value $\lambda^i k$ where λ defines the relationship between the start point P and a point ∅P and ∅ indicates a Frobenius Operation;

(vi) utilizing the resultant representation of the coordinate and the value $\lambda^i k$ as a session pair in a digital signature r,s where r is derived from the representation of a coordinate of a point on the curve and s is derived from the integer value associated with such point, the message to be signed and r.

13. A method of generating signature components for use in a digital signature scheme, said signature components including private information and a public key derived from said private information, said method comprising the steps of storing private information and related public key as an element in a set of such elements, cycling in a deterministic but unpredictable manner through said set to select at least one element of said set without repetition and utilizing said one element to derive a signature component in said digital signature scheme.

14. A method according to claim 13 wherein a pair of said elements are selected from said set and said pair of elements combined to provide said signature components.

15. A method according to claim 14 wherein one of said selected pair of elements is operated upon to produce private information and a public key derived from said one element prior to combination with the other of said elements.

16. A method according to claim 15 wherein a computation to combine said elements is initiated on one computing device and sufficient steps of said computation are performed on said one device to inhibit recognition of information in said elements and subsequent steps are performed on another computing device after transfer of a partially completed computation thereto.

17. A method according to claim 14 wherein said pairs of elements are selected by generating a pair of indices indicating respective locations of said elements in said set.

18. A method according to claim 17 wherein said indices are obtained from an ordered array arranged to provide each possible combination of indices.

19. A method according to claim 18 wherein said indices are selected from a counter that increments with each signature.

20. A method according to claim 19 wherein output from said counter is modified to provide a non-sequential selection of said indices.

21. A method of generating a digital signature implemented over an elliptic curve public key encryption scheme utilizing a session pair k, kP in which k is an integer maintained secret and kP represents a point on said curve resulting from a k-fold addition of starting point P, said method comprising the steps of storing a set of elements each having normal basis representation of a value of k and a normal basis representation of a value of kP in the field GF2^m, identifying each element of said set for subsequent retrieval, selecting a pair of said elements in a deterministic and unpredictable manner and combining said elements to provide a session pair for use in said digital signature.

09434247.110599

22. A method according to claim 21wherein an auxiliary transformation is performed on one of said elements selected prior to combination with the other thereof.

23. A method according to claim 22 wherein said elliptic curve is an anomalous curve and said auxiliary transformation is an application of a Frobenius Operator.

24. A method according to claim 23 wherein said auxiliary transformation includes an i-fold cyclic shift on said normal basis representation of said value kP associated with said element.

25. A method according to claim 24 wherein said pairs of elements are selected from an ordered grouping of pairs of the identifications of said elements.

26. A method according to claim 22 wherein combining of said elements includes a computation performed in part on one computing device and in part on another computing device.

09550117.743460

27. 27. A method according to claim 26 wherein sufficient steps of said computation are performed on said one computing device to inhibit identification of either of said elements.

28. 28. A method of generating a set of session pairs for use as a private key and a public key respectively in a public key cryptographic scheme, said method comprising the steps of establishing a set having a plurality of session pairs, selecting at least one of said session pairs, processing said selected session pair by applying a predetermined function thereto to generate a new session pair and incorporating said new session pair into said set.

29. A method according to claim 28 wherein said selection of said one of said session pairs is repeated a plurality of times.

30. A method according to claim 29 wherein a plurality of session pairs of said set is selected and combined to generate said new session pair.

31. A method according to claim 30 wherein said pairs are selected by a random number generator.

32. A method according to claim 31 wherein said selection of a plurality of pairs by said random number generator is repeated a plurality of times prior to said pairs being used to generate a private and public key pair.

33. A method according to claim 28 wherein said new session pairs are incorporated by accumulating said new session pair with an existing session pair.

34. A method according to claim 30 wherein an additional function is applied to at least one of said plurality of session pairs prior to combination with the other of said plurality of session pairs.

35. A method according to claim 30 wherein an additional function is applied after combination of said plurality session pairs to generate said new session pairs.

36. A method of generating a set of session pairs for use as a private key and a public key respectively in a public key cryptographic scheme, said method comprising the steps of establishing an initial set having a plurality of session pairs, selecting one of said pairs by a random selection process, and accumulating said selected pair with a randomly selected pair of said initial set.

37. A method according to claim 36 wherein successive selections and accumulations are performed on randomly selected ones of said set.

38. A method according to claim 37 wherein a function is applied to said selected one of said pairs prior to accumulation.

39. A method according to claim 37 wherein a random number generator is used to perform said random selections.

09434247 .110599